REMARKS

These remarks are set forth in response to the Non-Final Office Action. As this

amendment has been timely filed within the three-month statutory period, neither an extension of

time nor a fee is required. Presently, claims 1 through 13 are pending in the Patent Application.

Claims 1, 6, and 9 are independent claims. In the Office Action, claims 1 through 13 have been

rejected under 35 U.S.C. § 103(a) as being anticipated by U.S. Patent No. 6,081,900 to

Subramaniam et al. (Subramaniam). In response, the Applicants respectfully traverse the

rejections on the art as Subramaniam teaches tunneling non-hypertext transfer protocol (HTTP)

data through a reverse proxy <u>within HTTP messages</u> while the claims of the Patent Application

explicitly require that non-HTTP data is passed through the reverse proxy <u>without encapsulating</u>

<u>the non-HTTP data within HTTP messages</u>.

Prior to a discussion of the rejections on the art, a brief review of the Applicant's

invention will be helpful. The Applicant has invented is a method, system and apparatus for

tunneling non-HTTP streams through a reverse proxy. In the Applicants' invention, a socket

connection can be established with a reverse proxy. Based upon the establishment of the socket

connection, the socket can be passed to a non-HTTP data stream handler. The non-HTTP data

stream handler can maintain the open socket connection and can write non-HTTP data streams

over the socket <u>without encapsulating the non-HTTP data within an HTTP message</u>. The non-

HTTP data stream handler can continue to exchange the non-HTTP data over the open socket

until finished. Subsequently, the non-HTTP data stream handler can close the socket.

Significantly, and <u>unlike prior art HTTP tunneling implementations,</u> in the Applicants' invention,

the non-HTTP data can be exchanged over the secured connection without encapsulating the
non-HTTP data within HTTP messages.

Turning now to the rejections on the art, Subramaniam relates to securely accessing a
network from an external client. Requests for access to confidential data are redirected from a
target server to a border server, after which a secure sockets layer (SSL) connection between the
border server and the external client carries user authentication information. After the user is
authenticated to the network, requests may be redirected back to the original target server. Web
pages sent from the target server to the external client are scanned for non-secure uniform
resource locators (URLs) such as those containing the prefix "http://" and those URLs are
modified to make them secure. In one embodiment taught within Subramaniam, tunneling is
used for the redirection.

Figure 1 of Subramaniam is representative of the Subramaniam system. As shown in
Figure 1, secure data (shown as elements 134 and 138) is passed to a target server (shown as
element 104) through a border server (shown as element 106). The exchange of the secure data
from the border server to the target server is performed by using tunneling and is shown as
"Secure Data in Tunnel 138" within Figure 1. Figure 2 of Subramaniam clarifies the operation
of the system of Figure 1 by stating "transmit secure data from target server through border
server tunnel to user/client" in the method step labeled step 136 in Figure 2.

Importantly, as discussed in column 3, lines 40 through 50 of Subramaniam, column 3
line 66 through column 4, line 19 of Subramaniam, column 7, lines 1 through 35 of
Subramaniam, and column 8 lines 13 through 23 of Subramaniam, the border manager of the
Subramaniam system can re-write the URL of an incoming request associated with secure data

7

from an "http" header to a "https" header in order to invoke "HTTPS" treatment. As it is

understood in the art, HTTPS is HTTP over an SSL connection. The messages exchanged in

HTTPS are HTTP messages. The HTTP messages, however, are exchanged using SSL

connectivity.

Column 7, lines 24 through 35 of Subramaniam discuss the nature of HTTPS and

reference United States Patent No. 5,825,890 to Elgamal et al. (Elgamal). With specific

reference to Elgamal, it is stated with particularity:

> [T]he HTTPS header in the URL indicates that the server is a secure HTTP server. The "S" suffix
> in the header syntax indicates that the connection is to be a secure connection, and that the
> application should invoke the SSL library. The absence of an "S" from the header syntax, that is a
> normal HTTP header, would indicate that the connection need not be secure, and that the SSL
> library need not be invoked. Thus, the HTTPS header indicates to the application that the SSL
> library is to be called to provide a secure HTTP transfer. **Note that the protocol known as HTTP
> itself is not altered or modified,** Rather, information transferred between client and server
> applications is encrypted/decrypted in transit using the client side and server side SSL libraries. In
> effect, the SSL libraries provide an additional security layer between application and transport
> layers. See Elgamal column 14, line 55 through column 15, line 3 (emphasis added).

The emphasized portion of the Elgamal citation can be found on column 14, lines 64 through 65.

Considering the teachings of Subramaniam and Elgamal, in the claims of the Applicants'

Patent Application, it is explicitly required that "non-HTTP data" is written to a reverse proxy

"without encapsulating said non-HTTP data within HTTP messages". Clearly, the "without

encapsulating said non-HTTP data within HTTP messages" is not shown by Subramaniam

because Subramaniam requires the use of HTTP messages inherent to HTTP. Thus, the

Applicants respectfully believe that Subramaniam cannot be held to teach each and every recited

limitation of the claims of the Applicants' Patent Application.

The Examiner's present rejections differ from the previous rejections of the Non-Final

Office Action of June 29, 2005 in that Subramaniam no longer has been applied as art under 35

U.S.C. § 102(b), but as art under 35 U.S.C. § 103(a). In this regard, the Examiner has

recognized that Subramaniam fails to teach the encapsulation of non-HTTP data within an HTTP message in a reverse proxy. Nevertheless, the Examiner believes that the skilled artisan would modify Subramaniam to encapsulate non-HTTP data within an HTTP message in a reverse proxy because column 7, lines 65-67 of Subramaniam state, "FTP files, gopher resources, and other data on the target server 104 may be handled in a similar manner." Specifically, the Examiner stated, "Subramaniam et al. discloses one of ordinary skill in the art could use other protocols, such as FTP, for exchanging data."

The Applicants appreciate the Examiner's argument, but do not agree that the cited portion of Subramaniam--namely column 7, lines 65-67-- stands for the proposition that "non-HTTP data" is exchanged over the secure connection without encapsulating the non-HTTP data in an HTTP message. Rather, Subramaniam quite clearly contemplates that non-HTTP data is encapsulated within secure HTTP messages as stated in column 7, line 25. This stands in direct contradiction to the Applicants' claim language. More to the point, it is well known that an FTP server or gopher server can be accessed using HTTP in a Web browser such that the interface to the FTP server or gopher server is presented in HTML by way of HTTP. In these circumstances, non-HTTP data (FTP data for example) is encapsulated within HTTP messages. In the Applicants' claims, however, non-HTTP data is <u>not</u> encapsulated in HTTP messages even though the non-HTTP data is written to a reverse proxy.

For these reasons, the Applicant respectfully requests the withdrawal of the rejections under 35 U.S.C. § 103(a). This entire application is now believed to be in condition for allowance and such action is respectfully requested. The Applicants request that the Examiner call the undersigned if clarification is needed on any matter within this Amendment, or if the

Examiner believes a telephone interview would expedite the prosecution of the subject

application to completion.

Respectfully submitted,

Date: October 17, 2006

_____

Steven M. Greenberg, Reg. No.: 44,725
Attorney for Applicant(s)
Carey, Rodriguez, Greenberg & Paul, LLP
950 Peninsula Corporate Circle, Suite 3020
Boca Raton, Florida 33487
Customer No. 46321
Tel: (561) 922-3845
Fax: (561) 244-1062